CLAIMS

1. A method for securing, maintaining, monitoring and controlling computer files comprising:

    - providing a first data file, comprised of at least one first data file file name as well as a first data file hash value for each file referred to by each of said first data file file names;

    - providing a second data file, comprised of at least one second data file file name;

    - comparing said second data file to said first data file in a comparison cycle, wherein said comparison cycle further comprises;

        - obtaining each file referred to by each of said second data file file names;

        - generating a second data file hash value for each file referred to by each of said second data file file names;

        - sending each second data file hash value and each second data file file name to a comparison component.

2. A method as in claim 1 further comprising repeating the steps of:

    - obtaining each file referred to by each of said second data file file names;

- generating a second data file hash value for each file referred to by each of said second data file file names;

- sending each second data file hash value and each second data file file name to a comparison component.

3. A method as in claim 1 further comprising the step of:

- comparing each second data file hash value to each first data file hash value.

4. A method as in claim 1 wherein the step of providing a first data file further comprises proving a secure system data file.

5. A method as in claim 1 wherein the step of providing a first data file further comprises proving an alternate data file.

6. A method as in claim 1 further comprising the step of reporting the results of said comparison cycle.

7. A method as in claim 1 further comprising the step of logging the results of said comparison cycle.

8. A method as in claim 1 further comprising the step of sending the results of said comparison cycle to a client comparison status mechanism.

9. A method as in claim 1 wherein the step of generating a first data file further comprises using a Loop Back mechanism to generate said first data file.

10. The first data file generated by the method of claim 9.

11. A method for securing computer files comprising:

- generating a secure system data file, further comprising creating a hash value for a file and arranging said hash value with its respective file name;

- storing said secure system data file; and,

- comparing said secure system data file to a comparison data file in a comparison cycle, wherein said comparison data file further comprises at least one file name, and wherein said comparison cycle further comprises hashing said file name, and sending said hash value and file name to a comparison component, whereby said second data file hash value is compared to said first data file hash value.

12. A method as in claim 11 further comprising the step of reporting the results of said comparison cycle.

13. A method as in claim 11 further comprising the step of logging the results of said comparison cycle.

14. A method as in claim 11 further comprising the step of securing a system in lock down mode.

15. A method as in claim 11 further comprising the step of sending the results of said comparison cycle to a client comparison status mechanism.

16. A method as in claim 11 wherein the step of generating a secure system data file, further comprises using a Loop Back mechanism to generate said secure system data file.

17. The first data file generated by the method of claim 16.

18. An apparatus for securing, maintaining, monitoring and controlling computer files comprising:

- a first data file, comprised of at least one first data file file name as well as a first data file hash value for each file referred to by each of said first data file file names;

- a second data file, comprised of at least one second data file file name;

- whereby said second data file is compared to said first data file, by:

- a means for obtaining each file referred to by each of said second data file file names,

- a means for generating a second data file hash value for each file referred to by each of said second data file file names; and,

- a means for sending each second data file hash value and each second data file file name to a comparison component.

19. An apparatus as in claim 18 whereby said comparison component further comprises means for comparing each second data file hash value to each first data file hash value.

20. An apparatus as in claim 18 wherein said first data file further comprises a secure system data file.

21. An apparatus as in claim 18 wherein said first data file further comprises an alternate data file.

22. An apparatus as in claim 18 further comprising means for reporting the results of said comparison cycle.

23. An apparatus as in claim 18 further comprising means for logging the results of said comparison cycle.

24. An apparatus as in claim 18 further comprising means for sending the results of said comparison cycle to a client comparison status mechanism.

25. An apparatus as in claim 18 further comprising Loop Back mechanism means.

26. An apparatus as in claim 25 whereby said first data file is generated by said Loop Back mechanism means.